ELSEVIER

Journal of Computational and Applied Mathematics 62 (1995) 239–253

JOURNAL OF COMPUTATIONAL AND APPLIED MATHEMATICS

Quadratic congruential pseudorandom numbers: distribution of triples

Jürgen Eichenauer-Herrmann

Fachbereich Mathematik, Technische Hochschule Darmstadt, Schloßgartenstraße 7, D-64289 Darmstadt, Germany

Received 27 July 1994

Abstract

The present paper deals with the quadratic congruential method with power of two modulus for generating uniform pseudorandom numbers. Statistical independence properties of pairs and triples of successive terms in the generated sequences are studied based on the discrepancy of the corresponding point sets. In the main part of the paper a known upper bound for the discrepancy of pairs is improved and new upper bounds for the discrepancy of triples are established. Known lower bounds for the corresponding discrepancies are recalled. The method of proof relies on a detailed discussion of the properties of certain exponential sums.

Keywords: Uniform pseudorandom numbers; Quadratic congruential method; Power of two modulus; Statistical independence; Discrepancy of pairs and triples; Exponential sums

1. Introduction

Nonlinear congruential methods of generating uniform pseudorandom numbers in the interval $[0, 1)$ have been studied intensively during the last years. A review of the development of this important area can be found in the survey articles [3, 4, 6, 13–15, 17] and in the excellent monograph [16]. The oldest nonlinear congruential approach is the *quadratic congruential method* proposed in [9, p. 25], which recently received considerable attention [1, 2, 5, 7]. The present paper concentrates on the particularly important case of a power of two modulus $m = 2^\omega$ with some integer $\omega \geqslant 5$. Let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ for integers $n \geqslant 1$. For *parameters* $a, b, c \in \mathbb{Z}_m$ a *quadratic congruential sequence* $(y_n)_{n \geqslant 0}$ of elements of $\mathbb{Z}_m$ is defined by

$$y_{n+1} \equiv a y_n^2 + b y_n + c \,(\mathrm{mod}\, m), \quad n \geqslant 0.$$

A sequence $(x_n)_{n \geqslant 0}$ of *quadratic congruential pseudorandom numbers* in the interval $[0, 1)$ is obtained by $x_n = y_n/m$ for $n \geqslant 0$. The sequences $(x_n)_{n \geqslant 0}$ and $(y_n)_{n \geqslant 0}$ are purely periodic with the maximum possible period length m if and only if the conditions $a \equiv 0 \,(\mathrm{mod}\, 2)$, $b \equiv a + 1 \,(\mathrm{mod}\, 4)$, and $c \equiv 1 \,(\mathrm{mod}\, 2)$ are satisfied [9, p. 34]. The results in [7] on the statistical independence of pairs

SSDI 0377-0427(94)00105-7

of quadratic congruential pseudorandom numbers suggest that it is reasonable to choose the parameters a, b in such a way that $a \equiv 2 \pmod 4$ and $b \equiv 3 \pmod 4$.

Statistical independence properties of the generated sequences, which are very important for their usability in a stochastic simulation, can be analysed based on the discrepancy of s-tuples of successive pseudorandom numbers with $s \geqslant 2$. For N arbitrary points $\boldsymbol{t}_0, \boldsymbol{t}_1, \ldots, \boldsymbol{t}_{N-1} \in [0,1)^s$ their *discrepancy* is defined by

$$D_N(\boldsymbol{t}_0, \boldsymbol{t}_1, \ldots, \boldsymbol{t}_{N-1}) = \sup_J |F_N(J) - V(J)|,$$

where the supremum is extended over all subintervals J of $[0,1)^s$, $F_N(J)$ is N^{-1} times the number of points among $\boldsymbol{t}_0, \boldsymbol{t}_1, \ldots, \boldsymbol{t}_{N-1}$ falling into J, and $V(J)$ denotes the s-dimensional volume of J. Observe that the discrepancy of N true random points in $[0,1)^s$ is almost always of an order of magnitude $N^{-1/2}(\log\log N)^{1/2}$ according to the law of the iterated logarithm for discrepancies [8]. Subsequently, the abbreviations

$$\boldsymbol{x}_n = (x_n, x_{n+1}, \ldots, x_{n+s-1}) \in [0,1)^s, \quad n \geqslant 0,$$

and

$$D^{(s)}_{m;a,b,c} = D_m(\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_{m-1})$$

are used. Section 4 of the present paper contains upper and lower bounds for the discrepancy $D^{(2)}_{m;a,b,c}$ of pairs, which are based on earlier results in [7]. In Section 5 the main results of the present paper on the discrepancy $D^{(3)}_{m;a,b,c}$ of triples are established and discussed. Their proof relies on the analysis of certain exponential sums, which is carried out in Section 3. The reader is referred to [10] for an introduction to the theory of exponential sums. Section 2 contains some basic auxiliary results.

2. Auxiliary results

First, some further notation is necessary. For integers $k \geqslant 1$ and $q \geqslant 2$ let $C_k(q)$ be the set of all nonzero lattice points $(h_1, \ldots, h_k) \in \mathbb{Z}^k$ with $-q/2 < h_j \leqslant q/2$ for $1 \leqslant j \leqslant k$. Define

$$r(h,q) = \begin{cases} q \sin(\pi |h|/q) & \text{for } h \in C_1(q), \\ 1 & \text{for } h = 0, \end{cases}$$

and

$$r(\boldsymbol{h}, q) = \prod_{j=1}^{k} r(h_j, q)$$

for $\boldsymbol{h} = (h_1, \ldots, h_k) \in C_k(q)$. For real t the abbreviation $e(t) = \mathrm{e}^{2\pi i t}$ is used, and $\boldsymbol{u} \cdot \boldsymbol{v}$ stands for the standard inner product of $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{R}^k$. Subsequently, a known general result for estimating discrepancies is stated which follows from [11, Lemma 2.2], [16, Theorem 3.10].

Lemma 1. *Let $N \geqslant 1$ and $q \geqslant 2$ be integers. Let $\boldsymbol{t}_n = \boldsymbol{y}_n/q \in [0,1)^k$ with $\boldsymbol{y}_n \in \{0, 1, \ldots, q-1\}^k$ for $0 \leqslant n < N$. Then the discrepancy of the points $\boldsymbol{t}_0, \boldsymbol{t}_1, \ldots, \boldsymbol{t}_{N-1}$ satisfies*

$$D_N(\boldsymbol{t}_0, \boldsymbol{t}_1, \ldots, \boldsymbol{t}_{N-1}) \leqslant \frac{k}{q} + \frac{1}{N} \sum_{\boldsymbol{h} \in C_k(q)} \frac{1}{r(\boldsymbol{h}, q)} \left| \sum_{n=0}^{N-1} e(\boldsymbol{h} \cdot \boldsymbol{t}_n) \right|.$$

The following result is essentially due to Niederreiter [11, 12]. Its first part follows from [11, Lemma 2.3]; its second and fourth parts can be deduced from [12, Lemma 4], whereas the third part can be shown analogously.

Lemma 2. *Let* $\alpha \geqslant 1$ *and* $c \equiv 1 \pmod 2$ *be integers. Then*

$$\sum_{h \in C_1(2^\alpha)} \frac{1}{r(h, 2^\alpha)} < \frac{2}{\pi} \log 2^\alpha + \frac{2}{5},$$

$$\sum_{\substack{h \in C_1(2^\alpha) \\ h \equiv 1 \pmod 2}} \frac{1}{r(h, 2^\alpha)} < \frac{1}{\pi} \log 2^\alpha + \frac{5}{9}$$

for $\alpha \geqslant 3$,

$$\sum_{\substack{h \in C_1(2^\alpha) \\ h \equiv c \pmod 4}} \frac{1}{r(h, 2^\alpha)} < \frac{1}{2\pi} \log 2^\alpha + \frac{2}{7}$$

for $\alpha \geqslant 3$, *and*

$$\sum_{\substack{h \in C_1(2^\alpha) \\ h \equiv c \pmod 8}} \frac{1}{r(h, 2^\alpha)} < \frac{1}{4\pi} \log 2^\alpha + \frac{2}{7}$$

for $\alpha \geqslant 4$.

3. Exponential sums

For integers u, v, w, and $\alpha \geqslant 0$ an *exponential sum* is defined by

$$S(u, v, w; c; 2^\alpha) = \sum_{y \in \mathbb{Z}_{2^\alpha}} e((uy + v(ay^2 + by) + w(a^3y^4 + 2a^2by^3 + (2a^2c + ab^2 + ab)y^2 + (2abc + b^2)y))/2^\alpha),$$

where $a, b, c \in \mathbb{Z}$ with $a \equiv 2 \pmod 4$, $b \equiv 3 \pmod 4$, and $c \equiv 1 \pmod 2$. Some relevant properties of these sums are collected in the following three lemmas, where the abbreviation

$$\tau = \begin{cases} 0 & \text{for } v \equiv 1 \pmod 2, \\ 1 & \text{for } v \equiv 0 \pmod 2 \end{cases}$$

is used. First, observe that for $\alpha \leqslant 2 + \tau$ a straightforward calculation yields

$$S(u, v, w; c; 2^\alpha) = \sum_{y \in \mathbb{Z}_{2^\alpha}} e((u + v + 5w)y/2^\alpha) = \begin{cases} 2^\alpha & \text{for } u + v + 5w \equiv 0 \pmod{2^\alpha}, \\ 0 & \text{for } u + v + 5w \not\equiv 0 \pmod{2^\alpha}. \end{cases}$$

Lemma 3. *Let u, v, w, and $\alpha \geqslant 1$ be integers. If $u \equiv v \equiv w \equiv 0 \pmod 2$, then*

$$S(u,v,w;c;2^\alpha) = 2S(u/2, v/2, w/2; c; 2^{\alpha-1}).$$

Proof. It follows at once from $u \equiv v \equiv w \equiv 0 \pmod 2$ that

$$\begin{aligned} S(u,v,w;c;2^\alpha) &= 2 \sum_{y \in \mathbb{Z}_{2^{\alpha-1}}} e((uy + v(ay^2 + by) + w(a^3y^4 + 2a^2by^3 \\ &\qquad + (2a^2c + ab^2 + ab)y^2 + (2abc + b^2)y))/2^\alpha) \\ &= 2S(u/2, v/2, w/2; c; 2^{\alpha-1}). \qquad \square \end{aligned}$$

Lemma 4. *Let u, v, w, and $\alpha \geqslant 3 + \tau$ be integers. If $u - v + 5w \not\equiv 0 \pmod{2^{2+\tau}}$, then*

$$S(u,v,w;c;2^\alpha) = 0.$$

Proof. A short calculation shows that

$$\begin{aligned} S(u,v,w;c;2^\alpha) &= \sum_{y \in \mathbb{Z}_{2^{\alpha-2-\tau}}} \sum_{z \in \mathbb{Z}_{2^{2+\tau}}} e((u(y + 2^{\alpha-2-\tau}z) + v(ay^2 + by - 2^{\alpha-2-\tau}z) \\ &\qquad + w(a^3y^4 + 2a^2by^3 + (2a^2c + ab^2 + ab)y^2 + (2abc + b^2)y \\ &\qquad + 2^{\alpha-2-\tau}5z))/2^\alpha) \\ &= \sum_{y \in \mathbb{Z}_{2^{\alpha-2-\tau}}} e((uy + v(ay^2 + by) + w(a^3y^4 + 2a^2by^3 + (2a^2c + ab^2 + ab)y^2 \\ &\qquad + (2abc + b^2)y))/2^\alpha) \sum_{z \in \mathbb{Z}_{2^{2+\tau}}} e((u - v + 5w)z/2^{2+\tau}). \end{aligned}$$

Hence, it follows from $u - v + 5w \not\equiv 0 \pmod{2^{2+\tau}}$ that the last sum is zero, which yields the desired result. $\square$

Lemma 5. *Let u, v, w, and $\alpha \geqslant 3 + \tau$ be integers. If $(u,v,w) \not\equiv (0,0,0) \pmod 2$ and $u - v + w \equiv 4 \pmod{2^{2+\tau}}$, then*

$$\sum_{\substack{c \in \mathbb{Z}_{2^\alpha} \\ c \equiv 1 \pmod 2}} |S(u,v,w;c;2^\alpha)|^2 = 2^{2\alpha+\tau+1}.$$

Proof. Let $\nu \in \{0, 1, \ldots, \alpha - 3\}$ be defined by $\gcd(w, 2^{\alpha-3}) = 2^\nu$. Observe that $\gcd(v, 2^{\nu+1}) = 2^\tau$, since $v \equiv 0 \pmod 2$ implies that $w \equiv 1 \pmod 2$ and hence $\nu = 0$. Now, straightforward calculations show that

$$\begin{aligned} &\sum_{\substack{c \in \mathbb{Z}_{2^\alpha} \\ c \equiv 1 \pmod 2}} |S(u,v,w;c;2^\alpha)|^2 \\ &= \sum_{d \in \mathbb{Z}_{2^{\alpha-1}}} \sum_{y,z \in \mathbb{Z}_{2^\alpha}} e((u(y - z) + v(a(y^2 - z^2) + b(y - z)) \end{aligned}$$

$$+ w(a^3(y^4 - z^4) + 2a^2b(y^3 - z^3) + (2a^2(2d + 1) + ab^2 + ab)(y^2 - z^2)$$
$$+ (2ab(2d + 1) + b^2)(y - z)))/2^\alpha)$$

$$= \sum_{y,z \in \mathbb{Z}_{2^\alpha}} e((u(y - z) + v(a(y^2 - z^2) + b(y - z))$$
$$+ w(a^3(y^4 - z^4) + 2a^2b(y^3 - z^3) + (2a^2 + ab^2 + ab)(y^2 - z^2)$$
$$+ (2ab + b^2)(y - z)))/2^\alpha) \sum_{d \in \mathbb{Z}_{2^{\alpha-1}}} e(2aw(a(y + z) + b)(y - z)d/2^{\alpha-1})$$

$$= 2^{\alpha-1} \sum_{\substack{y,z \in \mathbb{Z}_{2^\alpha} \\ y \equiv z \,(\mathrm{mod}\, 2^{\alpha-\nu-3})}} e((u(y - z) + v(a(y^2 - z^2) + b(y - z))$$
$$+ w(a^3(y^4 - z^4) + 2a^2b(y^3 - z^3) + (2a^2 + ab^2 + ab)(y^2 - z^2)$$
$$+ (2ab + b^2)(y - z)))/2^\alpha)$$

$$= 2^{\alpha-1} \sum_{\substack{y,z \in \mathbb{Z}_{2^\alpha} \\ y \equiv z \,(\mathrm{mod}\, 2^{\alpha-\nu-3})}} e((u(y - z) + v(a(y^2 - z^2) + b(y - z)) + 5w(y - z))/2^\alpha)$$

$$= 2^{\alpha-1} \sum_{x \in \mathbb{Z}_{2^{\nu+3}}} \sum_{z \in \mathbb{Z}_{2^\alpha}} e((ux + v(a(2xz + 2^{\alpha-\nu-3}x^2) + bx) + 5wx)/2^{\nu+3})$$

$$= 2^{\alpha-1} \sum_{x \in \mathbb{Z}_{2^{\nu+3}}} e((ux + 2^{\alpha-\nu-3}vax^2 + vbx + 5wx)/2^{\nu+3}) \sum_{z \in \mathbb{Z}_{2^\alpha}} e(vaxz/2^{\nu+2})$$

$$= 2^{2\alpha-1} \sum_{\substack{x \in \mathbb{Z}_{2^{\nu+3}} \\ x \equiv 0 \,(\mathrm{mod}\, 2^{\nu-\tau+1})}} e((u - v + w + 4)x/2^{\nu+3})$$

$$= 2^{2\alpha-1} \sum_{\xi \in \mathbb{Z}_{2^{2+\tau}}} e((u - v + w + 4)\xi/2^{2+\tau}) = 2^{2\alpha+\tau+1}$$

which is the desired result. □

4. Discrepancy of pairs

The present section deals with the discrepancy $D^{(2)}_{m;a,b,c}$ of the pairs

$$\boldsymbol{x}_n = (x_n, x_{n+1}) \in [0, 1)^2, \quad 0 \leqslant n < m,$$

of successive quadratic congruential pseudorandom numbers. The upper bound in Theorem 6 improves an earlier bound in [7, Theorem 1] by a factor of nearly eight. Its proof is based on results in [7]. The lower bound in Theorem 7 is cited from [7, p. 249].

Theorem 6. *The discrepancy $D^{(2)}_{m;a,b,c}$ of pairs in the quadratic congruential method satisfies*

$$D^{(2)}_{m;a,b,c} < \frac{2(4+\sqrt{2})}{7} m^{-1/2} \left(\frac{1}{\pi}\log m + \frac{4}{7}\right)^2 + \frac{2}{m}$$

for any parameters $a \equiv 2 \pmod 4$, $b \equiv 3 \pmod 4$, and $c \equiv 1 \pmod 2$.

Proof. First, Lemma 1 is applied with $k = 2$, $N = q = m$, and $t_n = x_n$ for $0 \leqslant n < m$. This yields

$$\begin{aligned} D^{(2)}_{m;a,b,c} &\leqslant \frac{2}{m} + \frac{1}{m} \sum_{\boldsymbol{h} \in C_2(m)} \frac{1}{r(\boldsymbol{h},m)} \left| \sum_{n=0}^{m-1} e(\boldsymbol{h}\cdot\boldsymbol{x}_n) \right| \\ &= \frac{2}{m} + \frac{1}{m} \sum_{\nu=0}^{\omega} \sum_{\substack{\boldsymbol{h}=(h_1,h_2)\in C_2(m) \\ \gcd(h_2,m)=2^\nu}} \frac{1}{r(\boldsymbol{h},m)} \left| \sum_{n=0}^{m-1} e(\boldsymbol{h}\cdot\boldsymbol{x}_n) \right| \\ &= \frac{2}{m} + \sum_{\substack{\boldsymbol{h}=(h_1,h_2)\in C_2(m) \\ h_2 \equiv 0 \,(\mathrm{mod}\, 2^{\omega-2}) \\ h_1 + h_2 = 0}} \frac{1}{r(\boldsymbol{h},m)} + \frac{2}{m^{1/2}} \sum_{\nu=0}^{\omega-3} 2^{\nu/2} \sum_{\substack{\boldsymbol{h}=(h_1,h_2)\in C_2(m) \\ \gcd(h_2,m)=2^\nu \\ h_1 \equiv h_2 \,(\mathrm{mod}\, 2^{\nu+2})}} \frac{1}{r(\boldsymbol{h},m)}, \end{aligned}$$

where the last equality follows at once from [7, Lemma 7]. Straightforward calculations show that

$$\sum_{\substack{\boldsymbol{h}=(h_1,h_2)\in C_2(m) \\ h_2 \equiv 0 \,(\mathrm{mod}\, 2^{\omega-2}) \\ h_1 + h_2 = 0}} \frac{1}{r(\boldsymbol{h},m)} = \frac{2}{(r(m/4,m))^2} + \frac{1}{(r(m/2,m))^2} = \frac{5}{m^2},$$

which implies that

$$\begin{aligned} D^{(2)}_{m;a,b,c} &\leqslant \frac{2}{m} + \frac{5}{m^2} + \frac{2}{m^{1/2}} \sum_{\nu=0}^{\omega-3} 2^{-3\nu/2} \sum_{\substack{\boldsymbol{g}=(g_1,g_2)\in C_2(2^{\omega-\nu}) \\ g_2 \equiv 1 \,(\mathrm{mod}\, 2) \\ g_1 \equiv g_2 \,(\mathrm{mod}\, 4)}} \frac{1}{r(\boldsymbol{g}, 2^{\omega-\nu})} \\ &= \frac{2}{m} + \frac{5}{m^2} + \frac{2}{m^{1/2}} \sum_{\nu=0}^{\omega-3} 2^{-3\nu/2} \sum_{\substack{g_2 \in C_1(2^{\omega-\nu}) \\ g_2 \equiv 1 \,(\mathrm{mod}\, 2)}} \frac{1}{r(g_2, 2^{\omega-\nu})} \sum_{\substack{g_2 \in C_1(2^{\omega-\nu}) \\ g_1 \equiv g_2 \,(\mathrm{mod}\, 4)}} \frac{1}{r(g_1, 2^{\omega-\nu})}. \end{aligned}$$

Hence, it follows from Lemma 2 that

$$\begin{aligned} D^{(2)}_{m;a,b,c} &< \frac{2}{m} + \frac{5}{m^2} + \frac{2}{m^{1/2}} \sum_{\nu=0}^{\omega-3} 2^{-3\nu/2} \left(\frac{1}{\pi}\log 2^{\omega-\nu} + \frac{5}{9}\right)\left(\frac{1}{2\pi}\log 2^{\omega-\nu} + \frac{2}{7}\right) \\ &< \frac{2}{m} + \frac{16}{m^2}\left(\frac{1}{\pi}\log 4 + \frac{5}{9}\right)\left(\frac{1}{2\pi}\log 4 + \frac{2}{7}\right) \\ &\quad + \frac{2}{m^{1/2}} \sum_{\nu=0}^{\omega-3} 2^{-3\nu/2} \left(\frac{1}{\pi}\log 2^{\omega-\nu} + \frac{5}{9}\right)\left(\frac{1}{2\pi}\log 2^{\omega-\nu} + \frac{2}{7}\right) \\ &= \frac{2}{m} + \frac{2}{m^{1/2}} \sum_{\nu=0}^{\omega-2} 2^{-3\nu/2} \left(\frac{1}{\pi}\log 2^{\omega-\nu} + \frac{5}{9}\right)\left(\frac{1}{2\pi}\log 2^{\omega-\nu} + \frac{2}{7}\right) \end{aligned}$$

$$< \frac{2}{m} + \frac{2}{m^{1/2}} \sum_{v=0}^{\omega-2} 2^{-3v/2} \left(\frac{1}{\pi}\log m + \frac{5}{9}\right)\left(\frac{1}{2\pi}\log m + \frac{2}{7}\right)$$

$$< \frac{2}{m} + \frac{2}{m^{1/2}} \sum_{v=0}^{\infty} (2^{-3/2})^{v} \left(\frac{1}{\pi}\log m + \frac{5}{9}\right)\left(\frac{1}{2\pi}\log m + \frac{2}{7}\right)$$

$$= \frac{2}{m} + \frac{2(4+\sqrt{2})}{7m^{1/2}} \left(\frac{1}{\pi}\log m + \frac{5}{9}\right)\left(\frac{1}{\pi}\log m + \frac{4}{7}\right)$$

$$< \frac{2}{m} + \frac{2(4+\sqrt{2})}{7m^{1/2}} \left(\frac{1}{\pi}\log m + \frac{4}{7}\right)^{2}$$

which yields the desired result. □

Theorem 7. *The discrepancy $D^{(2)}_{m;a,b,c}$ of pairs in the quadratic congruential method satisfies*

$$D^{(2)}_{m;a,b,c} \geqslant \frac{1}{3(\pi+2)} m^{-1/2}$$

for any parameters $a \equiv 2 (\mathrm{mod}\, 4)$, $b \equiv 3 (\mathrm{mod}\, 4)$, and $c \equiv 1 (\mathrm{mod}\, 2)$.

Theorem 6 shows that $D^{(2)}_{m;a,b,c} = O(m^{-1/2}(\log m)^2)$ for any quadratic congruential sequence, where the implied constant is absolute. In particular, this upper bound is independent of the specific choice of the parameters a, b, c in the quadratic congruential method, provided the conditions $a \equiv 2 (\mathrm{mod}\, 4)$, $b \equiv 3 (\mathrm{mod}\, 4)$, and $c \equiv 1 (\mathrm{mod}\, 2)$ are met. Theorem 7 implies that the upper bound is best possible up to the logarithmic factor, since the discrepancy $D^{(2)}_{m;a,b,c}$ of any quadratic congruential generator with $a \equiv 2 (\mathrm{mod}\, 4)$, $b \equiv 3 (\mathrm{mod}\, 4)$, and $c \equiv 1 (\mathrm{mod}\, 2)$ has an order of magnitude at least $m^{-1/2}$. Altogether, Theorems 6 and 7 show that the discrepancy of pairs is always of an order of magnitude between $m^{-1/2}$ and $m^{-1/2}(\log m)^2$, which fits well the law of the iterated logarithm for the discrepancy of true random points in $[0, 1)^2$.

5. Discrepancy of triples

In this final section the discrepancy $D^{(3)}_{m;a,b,c}$ of the triples

$$x_n = (x_n, x_{n+1}, x_{n+2}) \in [0, 1)^3, \quad 0 \leqslant n < m,$$

of successive quadratic congruential pseudorandom numbers is studied. The main result of the present paper is Theorem 8, which provides an upper bound for the average value of the discrepancy of triples over the parameter c. Theorem 9 is an immediate consequence of this result. A proof is added for the sake of completeness. Theorem 10 corresponds to the main result in [5].

Theorem 8. *The average value of the discrepancy* $D^{(3)}_{m;a,b,c}$ *of triples in the quadratic congruential method over* $c \in \mathbb{Z}_m$ *with* $c \equiv 1 \pmod 2$ *satisfies*

$$\frac{2}{m} \sum_{\substack{c \in \mathbb{Z}_m \\ c \equiv 1 \pmod 2}} D^{(3)}_{m;a,b,c} < \frac{4(17+6\sqrt{2})}{31} m^{-1/2} \left(\frac{1}{\pi} \log m + \frac{11}{13} \right)^3 + \frac{3}{m}$$

for any parameters $a \equiv 2 \pmod 4$ *and* $b \equiv 3 \pmod 4$.

Proof. First, Lemma 1 is applied with $k = 3$, $N = q = m$, and $t_n = x_n$ for $0 \leqslant n < m$. This yields

$$D^{(3)}_{m;a,b,c} \leqslant \frac{3}{m} + \frac{1}{m} \sum_{\boldsymbol{h} \in C_3(m)} \frac{1}{r(\boldsymbol{h}, m)} \left| \sum_{n=0}^{m-1} e(\boldsymbol{h} \cdot \boldsymbol{x}_n) \right|.$$

Since $\boldsymbol{x}_n = (y_n, y_{n+1}, y_{n+2})/m$ and $y_{n+1} \equiv a y_n^2 + b y_n + c \pmod m$ for $n \geqslant 0$, it follows fron $\{y_0, y_1, \ldots, y_{m-1}\} = \mathbb{Z}_m$ that

$$\begin{aligned} \left| \sum_{n=0}^{m-1} e(\boldsymbol{h} \cdot \boldsymbol{x}_n) \right| &= \Bigg| \sum_{n=0}^{m-1} e((h_1 y_n + h_2(a y_n^2 + b y_n + c) \\ &\qquad + h_3(a(a y_n^2 + b y_n + c)^2 + b(a y_n^2 + b y_n + c) + c))/m) \Bigg| \\ &= |S(h_1, h_2, h_3; c; m)| \end{aligned}$$

for any $\boldsymbol{h} = (h_1, h_2, h_3) \in C_3(m)$, where S is the exponential sum of Section 3. Hence, one obtains

$$\begin{aligned} D^{(3)}_{m;a,b,c} &\leqslant \frac{3}{m} + \frac{1}{m} \sum_{\boldsymbol{h} = (h_1, h_2, h_3) \in C_3(m)} \frac{1}{r(\boldsymbol{h}, m)} |S(h_1, h_2, h_3; c; m)| \\ &= \frac{3}{m} + \frac{1}{m} \sum_{\nu=0}^{\omega-1} \sum_{\substack{\boldsymbol{h} = (h_1, h_2, h_3) \in C_3(m) \\ \gcd(h_1, h_2, h_3, m) = 2^\nu}} \frac{1}{r(\boldsymbol{h}, m)} |S(h_1, h_2, h_3; c; m)| \\ &= \frac{3}{m} + \frac{1}{m} \sum_{\nu=0}^{\omega-1} 2^\nu \sum_{\substack{\boldsymbol{g} = (g_1, g_2, g_3) \in C_3(2^{\omega-\nu}) \\ \gcd(g_1, g_2, g_3, 2) = 1}} \frac{1}{r(2^\nu \boldsymbol{g}, m)} |S(g_1, g_2, g_3; c; 2^{\omega-\nu})|, \end{aligned}$$

where in the last step Lemma 3 has been applied. Straightforward calculations show that

$$\begin{aligned} &\frac{1}{m} 2^{\omega-1} \sum_{\substack{\boldsymbol{g} = (g_1, g_2, g_3) \in C_3(2) \\ \gcd(g_1, g_2, g_3, 2) = 1}} \frac{1}{r(2^{\omega-1} \boldsymbol{g}, m)} |S(g_1, g_2, g_3; c; 2)| \\ &\quad = \sum_{\substack{\boldsymbol{g} = (g_1, g_2, g_3) \in C_3(2) \\ g_1 + g_2 + g_3 \equiv 0 \pmod 2}} \frac{1}{r(2^{\omega-1} \boldsymbol{g}, m)} = \frac{3}{(r(m/2, m))^2} = \frac{3}{m^2}, \end{aligned}$$

$$\frac{1}{m}2^{\omega-2}\sum_{\substack{\boldsymbol{g}=(g_1,g_2,g_3)\in C_3(4)\\ \gcd(g_1,g_2,g_3,2)=1}}\frac{1}{r(2^{\omega-2}\boldsymbol{g},m)}|S(g_1,g_2,g_3;c;4)|$$

$$=\sum_{\substack{\boldsymbol{g}=(g_1,g_2,g_3)\in C_3(4)\\ \gcd(g_1,g_2,g_3,2)=1\\ g_1+g_2+g_3\equiv 0\,(\mathrm{mod}\,4)}}\frac{1}{r(2^{\omega-2}\boldsymbol{g},m)}$$

$$=\frac{6}{(r(m/4,m))^2}+\frac{6}{(r(m/4,m))^2 r(m/2,m)}=\frac{12}{m^2}+\frac{12}{m^3},$$

and

$$\frac{1}{m}2^{\omega-3}\sum_{\substack{\boldsymbol{g}=(g_1,g_2,g_3)\in C_3(8)\\ \gcd(g_1,g_2,g_3,2)=1\\ g_2\equiv 0\,(\mathrm{mod}\,2)}}\frac{1}{r(2^{\omega-3}\boldsymbol{g},m)}|S(g_1,g_2,g_3;c;8)|$$

$$=\sum_{\substack{\boldsymbol{g}=(g_1,g_2,g_3)\in C_3(8)\\ g_1\equiv g_3\equiv 1\,(\mathrm{mod}\,2)\\ g_1+g_2+5g_3\equiv 0(\mathrm{mod}\,8)}}\frac{1}{r(2^{\omega-3}\boldsymbol{g},m)}$$

$$=\frac{4}{r(m/8,m)r(3m/8,m)}+\frac{2}{r(m/4,m)}\left(\frac{1}{r(m/8,m)}+\frac{1}{r(3m/8,m)}\right)^2$$

$$+\frac{2}{(r(m/8,m))^2 r(m/2,m)}+\frac{2}{(r(3m/8,m))^2 r(m/2,m)}$$

$$=\frac{8\sqrt{2}}{m^2}+\frac{16\sqrt{2}+32}{m^3},$$

which implies that

$$D^{(3)}_{m;a,b,c}\leqslant\frac{3}{m}+\frac{8\sqrt{2}+15}{m^2}+\frac{16\sqrt{2}+44}{m^3}$$

$$+\frac{1}{m}\sum_{\nu=0}^{\omega-3}2^{\nu}\sum_{\substack{\boldsymbol{g}=(g_1,g_2,g_3)\in C_3(2^{\omega-\nu})\\ g_2\equiv 1\,(\mathrm{mod}\,2)}}\frac{1}{r(2^{\nu}\boldsymbol{g},m)}|S(g_1,g_2,g_3;c;2^{\omega-\nu})|$$

$$+\frac{1}{m}\sum_{\nu=0}^{\omega-4}2^{\nu}\sum_{\substack{\boldsymbol{g}=(g_1,g_2,g_3)\in C_3(2^{\omega-\nu})\\ g_2\equiv 0\,(\mathrm{mod}\,2)\\ \gcd(g_1,g_3,2)=1}}\frac{1}{r(2^{\nu}\boldsymbol{g},m)}|S(g_1,g_2,g_3;c;2^{\omega-\nu})|.$$

Now, it follows from Lemma 4 that

$$D^{(3)}_{m;a,b,c} \leqslant \frac{3}{m} + \frac{8\sqrt{2}+15}{m^2} + \frac{16\sqrt{2}+44}{m^3}$$

$$+ \frac{1}{m} \sum_{\nu=0}^{\omega-3} 2^{\nu} \sum_{\substack{g=(g_1,g_2,g_3)\in C_3(2^{\omega-\nu}) \\ g_2 \equiv 1 \pmod 2 \\ g_1 - g_2 + g_3 \equiv 0 \pmod 4}} \frac{1}{r(2^{\nu}\boldsymbol{g}, m)} |S(g_1, g_2, g_3; c; 2^{\omega-\nu})|$$

$$+ \frac{1}{m} \sum_{\nu=0}^{\omega-4} 2^{\nu} \sum_{\substack{g=(g_1,g_2,g_3)\in C_3(2^{\omega-\nu}) \\ g_1 \equiv g_3 \equiv 1 \pmod 2 \\ g_1 - g_2 + g_3 \equiv 4 \pmod 8}} \frac{1}{r(2^{\nu}\boldsymbol{g}, m)} |S(g_1, g_2, g_3; c; 2^{\omega-\nu})|.$$

Therefore the average value of the discrepancy $D^{(3)}_{m;a,b,c}$ over $c \in \mathbb{Z}_m$ with $c \equiv 1 \pmod 2$ satisfies

$$\frac{2}{m} \sum_{\substack{c\in\mathbb{Z}_m \\ c\equiv 1 \pmod 2}} D^{(3)}_{m;a,b,c} \leqslant \frac{3}{m} + \frac{8\sqrt{2}+15}{m^2} + \frac{16\sqrt{2}+44}{m^3}$$

$$+ \frac{1}{m} \sum_{\nu=0}^{\omega-3} 2^{\nu} \sum_{\substack{g=(g_1,g_2,g_3)\in C_3(2^{\omega-\nu}) \\ g_2 \equiv 1 \pmod 2 \\ g_1 - g_2 + g_3 \equiv 0 \pmod 4}} \frac{1}{r(2^{\nu}\boldsymbol{g}, m)}$$

$$\cdot \left(\frac{1}{2^{\omega-\nu-1}} \sum_{\substack{c\in\mathbb{Z}_{2^{\omega-\nu}} \\ c\equiv 1 \pmod 2}} |S(g_1, g_2, g_3; c; 2^{\omega-\nu})| \right)$$

$$+ \frac{1}{m} \sum_{\nu=0}^{\omega-4} 2^{\nu} \sum_{\substack{g=(g_1,g_2,g_3)\in C_3(2^{\omega-\nu}) \\ g_1 \equiv g_3 \equiv 1 \pmod 2 \\ g_1 - g_2 + g_3 \equiv 4 \pmod 8}} \frac{1}{r(2^{\nu}\boldsymbol{g}, m)}$$

$$\cdot \left(\frac{1}{2^{\omega-\nu-1}} \sum_{\substack{c\in\mathbb{Z}_{2^{\omega-\nu}} \\ c\equiv 1 \pmod 2}} |S(g_1, g_2, g_3; c; 2^{\omega-\nu})| \right)$$

$$\leqslant \frac{3}{m} + \frac{8\sqrt{2}+15}{m^2} + \frac{16\sqrt{2}+44}{m^3}$$

$$+ \frac{1}{m} \sum_{\nu=0}^{\omega-3} 2^{\nu} \sum_{\substack{g=(g_1,g_2,g_3)\in C_3(2^{\omega-\nu}) \\ g_2 \equiv 1 \pmod 2 \\ g_1 - g_2 + g_3 \equiv 0 \pmod 4}} \frac{1}{r(2^{\nu}\boldsymbol{g}, m)}$$

$$\cdot \sqrt{\frac{1}{2^{\omega-\nu-1}} \sum_{\substack{c\in\mathbb{Z}_{2^{\omega-\nu}} \\ c\equiv 1 \pmod 2}} |S(g_1, g_2, g_3; c; 2^{\omega-\nu})|^2}$$

$$+\frac{1}{m}\sum_{\nu=0}^{\omega-4}2^{\nu}\sum_{\substack{\boldsymbol{g}=(g_1,g_2,g_3)\in C_3(2^{\omega-\nu})\\ g_1\equiv g_3\equiv 1\,(\mathrm{mod}\,2)\\ g_1-g_2+g_3\equiv 4\,(\mathrm{mod}\,8)}}\frac{1}{r(2^{\nu}\boldsymbol{g},m)}$$

$$\cdot\sqrt{\frac{1}{2^{\omega-\nu-1}}\sum_{\substack{c\in\mathbb{Z}_{2^{\omega-\nu}}\\ c\equiv 1\,(\mathrm{mod}\,2)}}|S(g_1,g_2,g_3;c;2^{\omega-\nu})|^2},$$

where finally Schwarz's inequality has been applied. Now, Lemma 5 can be used in order to obtain

$$\frac{2}{m}\sum_{\substack{c\in\mathbb{Z}_m\\ c\equiv 1\,(\mathrm{mod}\,2)}}D^{(3)}_{m;a,b,c}\leqslant\frac{3}{m}+\frac{8\sqrt{2}+15}{m^2}+\frac{16\sqrt{2}+44}{m^3}$$

$$+\frac{2}{m^{1/2}}\sum_{\nu=0}^{\omega-3}2^{\nu/2}\sum_{\substack{\boldsymbol{g}=(g_1,g_2,g_3)\in C_3(2^{\omega-\nu})\\ g_2\equiv 1\,(\mathrm{mod}\,2)\\ g_1-g_2+g_3\equiv 0\,(\mathrm{mod}\,4)}}\frac{1}{r(2^{\nu}\boldsymbol{g},m)}$$

$$+\frac{2\sqrt{2}}{m^{1/2}}\sum_{\nu=0}^{\omega-4}2^{\nu/2}\sum_{\substack{\boldsymbol{g}=(g_1,g_2,g_3)\in C_3(2^{\omega-\nu})\\ g_1\equiv g_3\equiv 1\,(\mathrm{mod}\,2)\\ g_1-g_2+g_3\equiv 4\,(\mathrm{mod}\,8)}}\frac{1}{r(2^{\nu}\boldsymbol{g},m)}$$

$$=\frac{3}{m}+\frac{8\sqrt{2}+15}{m^2}+\frac{16\sqrt{2}+44}{m^3}$$

$$+\frac{4}{m^{1/2}}\sum_{\nu=0}^{\omega-3}2^{\nu/2}\sum_{\substack{\boldsymbol{g}=(g_1,g_2,g_3)\in C_3(2^{\omega-\nu})\\ g_1\equiv 0\,(\mathrm{mod}\,2)\\ g_2\equiv 1\,(\mathrm{mod}\,2)\\ g_3\equiv g_2-g_1\,(\mathrm{mod}\,4)}}\frac{1}{r(2^{\nu}\boldsymbol{g},m)}$$

$$+\frac{2\sqrt{2}}{m^{1/2}}\sum_{\nu=0}^{\omega-4}2^{\nu/2}\sum_{\substack{\boldsymbol{g}=(g_1,g_2,g_3)\in C_3(2^{\omega-\nu})\\ g_1\equiv 1\,(\mathrm{mod}\,2)\\ g_2\equiv 0\,(\mathrm{mod}\,2)\\ g_3\equiv g_2-g_1+4\,(\mathrm{mod}\,8)}}\frac{1}{r(2^{\nu}\boldsymbol{g},m)}$$

$$=\frac{3}{m}+\frac{8\sqrt{2}+15}{m^2}+\frac{16\sqrt{2}+44}{m^3}$$

$$+\frac{4}{m^{1/2}}\sum_{\nu=0}^{\omega-3}2^{-3\nu/2}\sum_{\substack{g_1\in C_1(2^{\omega-\nu})\cup\{0\}\\ g_1\equiv 0\,(\mathrm{mod}\,2)}}\frac{1}{r(2^{\nu}g_1,m)}$$

$$\cdot\sum_{\substack{g_2\in C_1(2^{\omega-\nu})\\ g_2\equiv 1\,(\mathrm{mod}\,2)}}\frac{1}{r(g_2,2^{\omega-\nu})}\sum_{\substack{g_3\in C_1(2^{\omega-\nu})\\ g_3\equiv g_2-g_1\,(\mathrm{mod}\,4)}}\frac{1}{r(g_3,2^{\omega-\nu})}$$

$$+\frac{2\sqrt{2}}{m^{1/2}}\sum_{v=0}^{\omega-4}2^{-3v/2}\sum_{\substack{g_2\in C_1(2^{\omega-v})\cup\{0\}\\ g_2\equiv 0\,(\mathrm{mod}\,2)}}\frac{1}{r(2^v g_2,m)}$$

$$\cdot\sum_{\substack{g_1\in C_1(2^{\omega-v})\\ g_1\equiv 1\,(\mathrm{mod}\,2)}}\frac{1}{r(g_1,2^{\omega-v})}\sum_{\substack{g_3\in C_1(2^{\omega-v})\\ g_3\equiv g_2-g_1+4\,(\mathrm{mod}\,8)}}\frac{1}{r(g_3,2^{\omega-v})}.$$

Hence, it follows from Lemma 2 that

$$\frac{2}{m}\sum_{\substack{c\in\mathbb{Z}_m\\ c\equiv 1\,(\mathrm{mod}\,2)}}D^{(3)}_{m;a,b,c}<\frac{3}{m}+\frac{8\sqrt{2}+15}{m^2}+\frac{16\sqrt{2}+44}{m^3}$$

$$+\frac{4}{m^{1/2}}\sum_{v=0}^{\omega-3}2^{-3v/2}\sum_{\substack{g_1\in C_1(2^{\omega-v})\cup\{0\}\\ g_1\equiv 0\,(\mathrm{mod}\,2)}}\frac{1}{r(2^v g_1,m)}$$

$$\cdot\left(\frac{1}{\pi}\log 2^{\omega-v}+\frac{5}{9}\right)\left(\frac{1}{2\pi}\log 2^{\omega-v}+\frac{2}{7}\right)$$

$$+\frac{2\sqrt{2}}{m^{1/2}}\sum_{v=0}^{\omega-4}2^{-3v/2}\sum_{\substack{g_2\in C_1(2^{\omega-v})\cup\{0\}\\ g_2\equiv 0\,(\mathrm{mod}\,2)}}\frac{1}{r(2^v g_2,m)}$$

$$\cdot\left(\frac{1}{\pi}\log 2^{\omega-v}+\frac{5}{9}\right)\left(\frac{1}{4\pi}\log 2^{\omega-v}+\frac{2}{7}\right)$$

$$=\frac{3}{m}+\frac{8\sqrt{2}+15}{m^2}+\frac{16\sqrt{2}+44}{m^3}$$

$$+\frac{4}{m^{1/2}}\sum_{v=0}^{\omega-3}2^{-3v/2}\left(1+2^{-v-1}\sum_{h\in C_1(2^{\omega-v-1})}\frac{1}{r(h,2^{\omega-v-1})}\right)$$

$$\cdot\left(\frac{1}{\pi}\log 2^{\omega-v}+\frac{5}{9}\right)\left(\frac{1}{2\pi}\log 2^{\omega-v}+\frac{2}{7}\right)$$

$$+\frac{2\sqrt{2}}{m^{1/2}}\sum_{v=0}^{\omega-4}2^{-3v/2}\left(1+2^{-v-1}\sum_{h\in C_1(2^{\omega-v-1})}\frac{1}{r(h,2^{\omega-v-1})}\right)$$

$$\cdot\left(\frac{1}{\pi}\log 2^{\omega-v}+\frac{5}{9}\right)\left(\frac{1}{4\pi}\log 2^{\omega-v}+\frac{2}{7}\right)$$

$$<\frac{3}{m}+\frac{8\sqrt{2}+15}{m^2}+\frac{16\sqrt{2}+44}{m^3}$$

$$+\frac{4}{m^{1/2}}\sum_{v=0}^{\omega-3}2^{-3v/2}\left(1+2^{-v}\left(\frac{1}{\pi}\log 2^{\omega-v-1}+\frac{1}{5}\right)\right)$$

$$
\begin{aligned}
&\cdot\left(\frac{1}{\pi}\log 2^{\omega-\nu}+\frac{5}{9}\right)\left(\frac{1}{2\pi}\log 2^{\omega-\nu}+\frac{2}{7}\right)\\
&+\frac{2\sqrt{2}}{m^{1/2}}\sum_{\nu=0}^{\omega-4}2^{-3\nu/2}\left(1+2^{-\nu}\left(\frac{1}{\pi}\log 2^{\omega-\nu-1}+\frac{1}{5}\right)\right)\\
&\cdot\left(\frac{1}{\pi}\log 2^{\omega-\nu}+\frac{5}{9}\right)\left(\frac{1}{4\pi}\log 2^{\omega-\nu}+\frac{2}{7}\right)\\
<&\frac{3}{m}+\frac{64}{m^2}\left(1+\frac{8}{m}\left(\frac{1}{\pi}\log 4+\frac{1}{5}\right)\right)\left(\frac{1}{\pi}\log 8+\frac{5}{9}\right)\left(\frac{1}{4\pi}\log 8+\frac{2}{7}\right)\\
&+\frac{4}{m^{1/2}}\sum_{\nu=0}^{\omega-3}2^{-3\nu/2}\left(1+2^{-\nu}\left(\frac{1}{\pi}\log 2^{\omega-\nu-1}+\frac{1}{5}\right)\right)\\
&\cdot\left(\frac{1}{\pi}\log 2^{\omega-\nu}+\frac{5}{9}\right)\left(\frac{1}{2\pi}\log 2^{\omega-\nu}+\frac{2}{7}\right)\\
&+\frac{2\sqrt{2}}{m^{1/2}}\sum_{\nu=0}^{\omega-4}2^{-3\nu/2}\left(1+2^{-\nu}\left(\frac{1}{\pi}\log 2^{\omega-\nu-1}+\frac{1}{5}\right)\right)\\
&\cdot\left(\frac{1}{\pi}\log 2^{\omega-\nu}+\frac{5}{9}\right)\left(\frac{1}{4\pi}\log 2^{\omega-\nu}+\frac{2}{7}\right)\\
=&\frac{3}{m}+\frac{1}{m^{1/2}}\sum_{\nu=0}^{\omega-3}2^{-3\nu/2}\left(1+2^{-\nu}\left(\frac{1}{\pi}\log 2^{\omega-\nu-1}+\frac{1}{5}\right)\right)\\
&\cdot\left(\frac{1}{\pi}\log 2^{\omega-\nu}+\frac{5}{9}\right)\left(\frac{4+\sqrt{2}}{2\pi}\log 2^{\omega-\nu}+\frac{8+4\sqrt{2}}{7}\right)\\
<&\frac{3}{m}+\frac{1}{m^{1/2}}\sum_{\nu=0}^{\omega-3}2^{-3\nu/2}\left(1+2^{-\nu}\left(\frac{1}{\pi}\log m+\frac{1}{5}-\frac{\log 2}{\pi}\right)\right)\\
&\cdot\left(\frac{1}{\pi}\log m+\frac{5}{9}\right)\left(\frac{4+\sqrt{2}}{2\pi}\log m+\frac{8+4\sqrt{2}}{7}\right)\\
<&\frac{3}{m}+\frac{1}{m^{1/2}}\left(\sum_{\nu=0}^{\infty}(2^{-3/2})^{\nu}+\sum_{\nu=0}^{\infty}(2^{-5/2})^{\nu}\left(\frac{1}{\pi}\log m+\frac{1}{5}-\frac{\log 2}{\pi}\right)\right)\\
&\cdot\left(\frac{1}{\pi}\log m+\frac{5}{9}\right)\left(\frac{4+\sqrt{2}}{2\pi}\log m+\frac{8+4\sqrt{2}}{7}\right)\\
=&\frac{3}{m}+\frac{1}{m^{1/2}}\left(\frac{2(4+\sqrt{2})}{7}+\frac{4(8+\sqrt{2})}{31}\left(\frac{1}{\pi}\log m+\frac{1}{5}-\frac{\log 2}{\pi}\right)\right)\\
&\cdot\left(\frac{1}{\pi}\log m+\frac{5}{9}\right)\left(\frac{4+\sqrt{2}}{2\pi}\log m+\frac{8+4\sqrt{2}}{7}\right)
\end{aligned}
$$

$$= \frac{3}{m} + \frac{4(17+6\sqrt{2})}{31m^{1/2}}\left(\frac{1}{\pi}\log m + \frac{1}{5} - \frac{\log 2}{\pi} + \frac{15+2\sqrt{2}}{14}\right)$$

$$\cdot\left(\frac{1}{\pi}\log m + \frac{5}{9}\right)\left(\frac{1}{\pi}\log m + \frac{8(3+\sqrt{2})}{49}\right)$$

$$< \frac{3}{m} + \frac{4(17+6\sqrt{2})}{31m^{1/2}}\left(\frac{1}{\pi}\log m + \frac{11}{13}\right)^3$$

which yields the desired result. □

Theorem 9. *Let the parameters* $a \equiv 2 \pmod 4$ *and* $b \equiv 3 \pmod 4$ *be fixed. Let* $0 < \alpha \leqslant 1$. *Then there exist more than* $(1-\alpha)m/2$ *values of* $c \in \mathbb{Z}_m$ *with* $c \equiv 1 \pmod 2$ *such that the discrepancy* $D^{(3)}_{m;a,b,c}$ *of triples in the quadratic congruential method satisfies*

$$D^{(3)}_{m;a,b,c} < \frac{1}{\alpha}\left(\frac{4(17+6\sqrt{2})}{31}m^{-1/2}\left(\frac{1}{\pi}\log m + \frac{11}{13}\right)^3 + \frac{3}{m}\right).$$

Proof. Subsequently, the abbreviation

$$M = \frac{4(17+6\sqrt{2})}{31}m^{-1/2}\left(\frac{1}{\pi}\log m + \frac{11}{13}\right)^3 + \frac{3}{m}$$

is used. Suppose that there exist at most $(1-\alpha)m/2$ values of $c \in \mathbb{Z}_m$ with $c \equiv 1 \pmod 2$ and $D^{(3)}_{m;a,b,c} < \alpha^{-1}M$, i.e., there exist at least $\alpha m/2$ values of $c \in \mathbb{Z}_m$ with $c \equiv 1 \pmod 2$ and $D^{(3)}_{m;a,b,c} \geqslant \alpha^{-1}M$. Hence, one obtains

$$\sum_{\substack{c \in \mathbb{Z}_m \\ c \equiv 1 \pmod 2}} D^{(3)}_{m;a,b,c} \geqslant Mm/2,$$

which contradicts Theorem 8. □

Theorem 10. *Let* $\omega = 3v + \mu + 2$ *for suitable integers* $v \geqslant 1$ *and* $\mu \in \{0,1,2\}$. *Let* $a \equiv 2 \pmod 4$, $b \equiv 3 \pmod 4$, *and* $c \equiv 1 \pmod 2$ *be parameters with* $(b-3)(b+1) \equiv 4ac \pm 8 + 2^{2v+4} \pmod{2^{\omega-v+1}}$. *Then the discrepancy* $D^{(3)}_{m;a,b,c}$ *of triples in the quadratic congruential method satisfies*

$$D^{(3)}_{m;a,b,c} \geqslant \frac{1}{2^{(7-\mu)/3}(\pi^2+3\pi+3)}m^{-1/3}.$$

Theorem 8 shows that for any parameters a, b the discrepancy $D^{(3)}_{m;a,b,c}$, on the average over the parameter c, has an order of magnitude at most $m^{-1/2}(\log m)^3$. In particular, this upper bound for the average value is independent of the specific choice of the parameters a, b in the quadratic congruential method, provided the conditions $a \equiv 2 \pmod 4$ and $b \equiv 3 \pmod 4$ are met. Theorem 7 implies that the upper bound for the average value is best possible up to the logarithmic factor, since the discrepancy $D^{(2)}_{m;a,b,c}$, and hence even more the discrepancy $D^{(3)}_{m;a,b,c}$, of any quadratic congruential generator with $a \equiv 2 \pmod 4$, $b \equiv 3 \pmod 4$, and $c \equiv 1 \pmod 2$ has an order of

magnitude at least $m^{-1/2}$. Altogether, these results show that the discrepancy of triples is of an order of magnitude between $m^{-1/2}$ and $m^{-1/2}(\log m)^3$, which again fits the law of the iterated logarithm for the discrepancy of true random points in $[0,1)^3$. Theorem 9 provides even more information, since it implies that for any parameters a, b only an arbitrarily small percentage of the parameters c may lead to a discrepancy of triples with an order of magnitude greater than $m^{-1/2}(\log m)^3$. On the other hand, Theorem 10 shows that there exist parameters a, b, c in the quadratic congruential method such that the discrepancy of triples is of an order of magnitude at least $m^{-1/3}$, which is too large in view of the law of the iterated logarithm. It is still an unsolved problem to identify all values of the parameters a, b, c, for which the discrepancy of triples is of an order of magnitude considerably greater than $m^{-1/2}$.

References

[1] J. Eichenauer and J. Lehn, On the structure of quadratic congruential sequences, *Manuscripta Math.* **58** (1987) 129–140.

[2] J. Eichenauer-Herrmann, A remark on the discrepancy of quadratic congruential pseudorandom numbers, *J. Comput. Appl. Math.* **43** (1992) 383–387.

[3] J. Eichenauer-Herrmann, Inversive congruential pseudorandom numbers: a tutorial, *Internat. Statist. Rev.* **60** (1992) 167–176.

[4] J. Eichenauer-Herrmann, Inversive congruential pseudorandom numbers, *Z. Angew. Math. Mech.* **73** (1993) T644–T647.

[5] J. Eichenauer-Herrmann, On the discrepancy of quadratic congruential pseudorandom numbers with power of two modulus, *J. Comput. Appl. Math.* **53** (3) (1994) 371–376.

[6] J. Eichenauer-Herrmann, Pseudorandom number generation by nonlinear methods, *Internat. Statist. Rev.*, to appear.

[7] J. Eichenauer-Herrmann and H. Niederreiter, On the discrepancy of quadratic congruential pseudorandom numbers, *J. Comput. Appl. Math.* **34** (1991) 243–249.

[8] J. Kiefer, On large deviations of the empiric d.f. of vector chance variables and a law of the iterated logarithm, *Pacific J. Math.* **11** (1961) 649–660.

[9] D.E. Knuth, *The Art of Computer Programming, Vol. 2, Seminumerical Algorithms* (Addison-Wesley, Reading, MA, 2nd ed., 1981).

[10] R. Lidl and H. Niederreiter, *Finite Fields* (Addison-Wesley, Reading, MA, 1983).

[11] H. Niederreiter, Pseudo-random numbers and optimal coefficients, *Adv. Math.* **26** (1977) 99–181.

[12] H. Niederreiter, The serial test for congruential pseudorandom numbers generated by inversions, *Math. Comp.* **52** (1989) 135–144.

[13] H. Niederreiter, Recent trends in random number and random vector generation, *Ann. Oper. Res.* **31** (1991) 323–346.

[14] H. Niederreiter, Nonlinear methods for pseudorandom number and vector generation, in: G. Pflug and U. Dieter, Eds., *Simulation and Optimization*, Lecture Notes in Economics and Mathematical Systems, Vol. 374 (Springer, Berlin, 1992) 145–153.

[15] H. Niederreiter, Finite fields, pseudorandom numbers, and quasirandom points, in: G.L. Mullen and P.J.-S. Shiue, Eds., *Finite Fields, Coding Theory, and Advances in Communications and Computing* (Dekker, New York, 1992) 375–394.

[16] H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods* (SIAM, Philadelphia, PA, 1992).

[17] H. Niederreiter, Pseudorandom numbers and quasirandom points, *Z. Angew. Math. Mech.* **73** (1993) T648–T652.